



ELECTRICAL
& COMPUTER
ENGINEERING

ECE-595 Network Softwarization

PROF. FABRIZIO GRANELLI (FABRIZIO.GRANELLI@UNITN.IT)

PROF. MICHAEL DEVETSIKOTIS (MDEVETS@UNM.EDU)



Cellular Networks

- Architecture
- Standards (GSM to LTE)
- Focus on LTE

Table of Contents

Wireless spectrum and cellular bands

Important cellular concepts

Overview of cellular standards

GSM, UMTS, and LTE:

- Network components, Architecture and Protocols

Focus on LTE

What is LTE

LTE is Long Term Evolution

Fourth generation cellular technology standard from the 3rd Generation Partnership Project (3GPP)

Deployed worldwide and installations are increasing

All implementations must meet baseline requirements

- Increased Speed
- Multiple Antennas (i.e., MIMO)
- IP-based network (All circuits are gone/fried!)
- New air interface: OFDMA (Orthogonal Frequency-Division Multiple Access)
- Also includes duplexing, timing, carrier spacing, coding...

LTE is always evolving and 3GPP often drops new “releases”

Cellular Network Operators

Telecommunications company (telco)

- Purchases spectrum
- Builds out network (base stations and backhaul network)
- Verizon, AT&T, T-Mobile, Sprint

Mobile Virtual Network Operator (MVNO)

- Does not have to purchase spectrum
- Rents the towers but runs a distinct network
- Cricket, Ting, MetroPCS, ...

Radio Frequency Spectrum

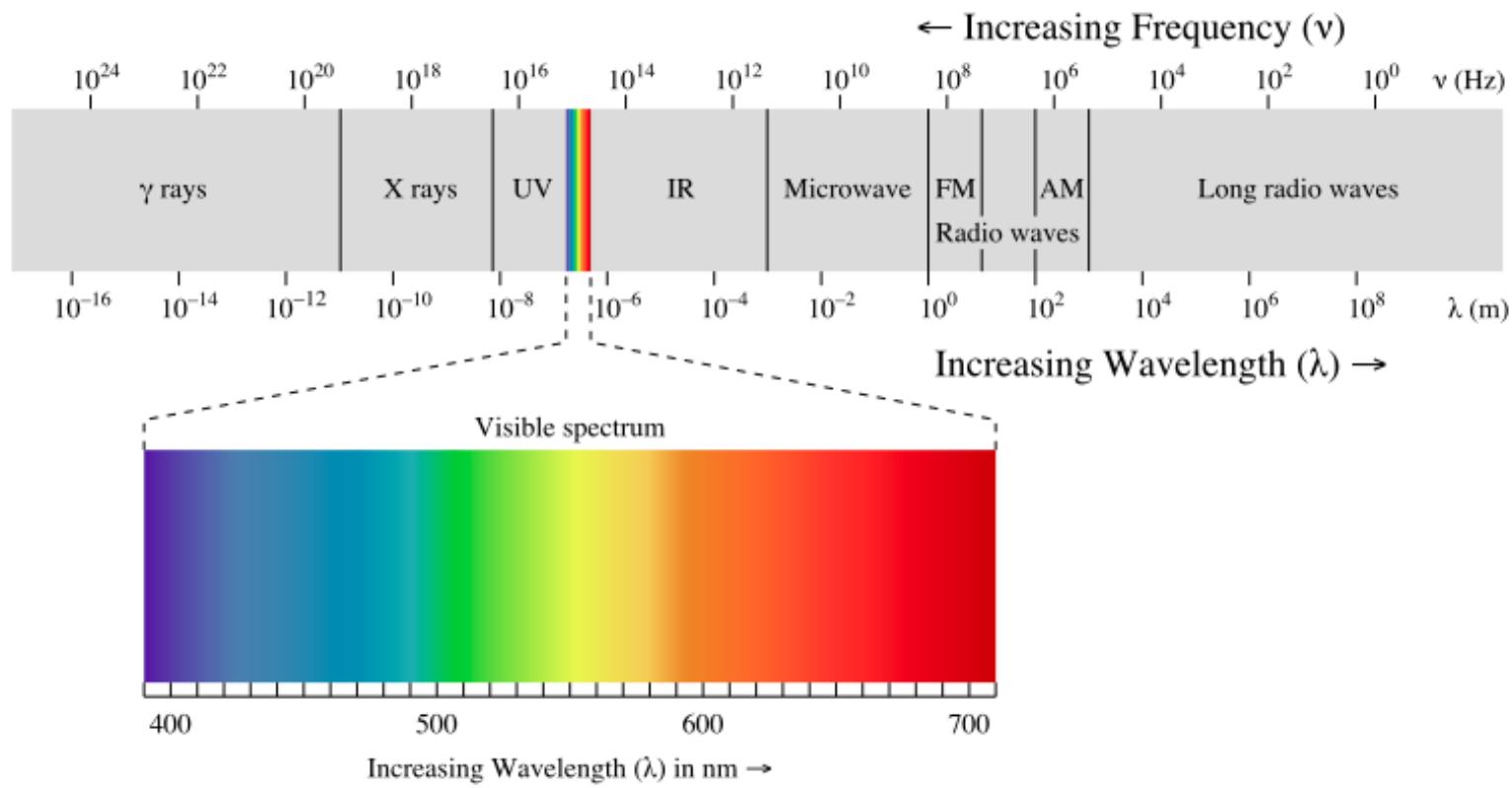
Describes a range of frequencies of electromagnetic waves used for communication and other purposes

RF energy is alternating current that, when channeled into an antenna, generates a specific electromagnetic field.

This field can be used for wireless communication

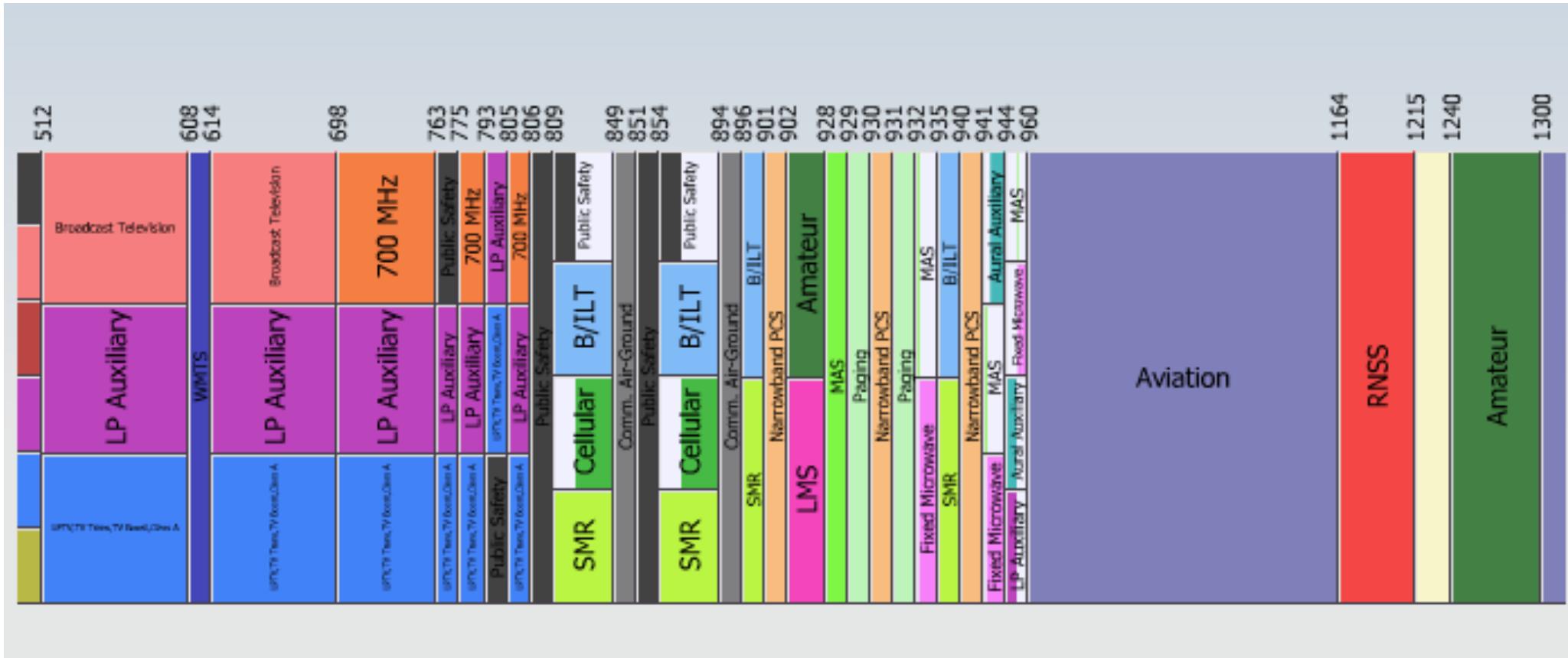
Typically, cellular spectrum ranges from 300 MHz to 3 GHz

EM Spectrum



Thanks to [Wikipedia](#)

Wireless Spectrum



From an interactive map available via the [FCC](#)

Popular Cellular Bands

700 Mhz Band (Blocks A - E)

- Considered uniquely useful to cellular activities
- Verizon, US Cellular, AT&T and others own various portions
- Will be used for 4G
- Includes reserved spectrum for public safety

850 MHz

- Great for cellular service
- Easily bounces off objects

1900 MHz band (PCS)

2100 MHZ (Blocks A - F)

- Mostly T-Mobile, but includes Cricket and MetroPCS

This information changes periodically as spectrum is purchased & released

Chipset

In the past, phones have typically been tied to a single carrier

A phone's hardware is tied to a carrier based on many things (like the IMEI), but the major ones are the cellular standard and frequencies the carrier uses

Phones are manufactured to work on specific radio frequencies

- Specific chips needed for a given frequency range, thus chipset

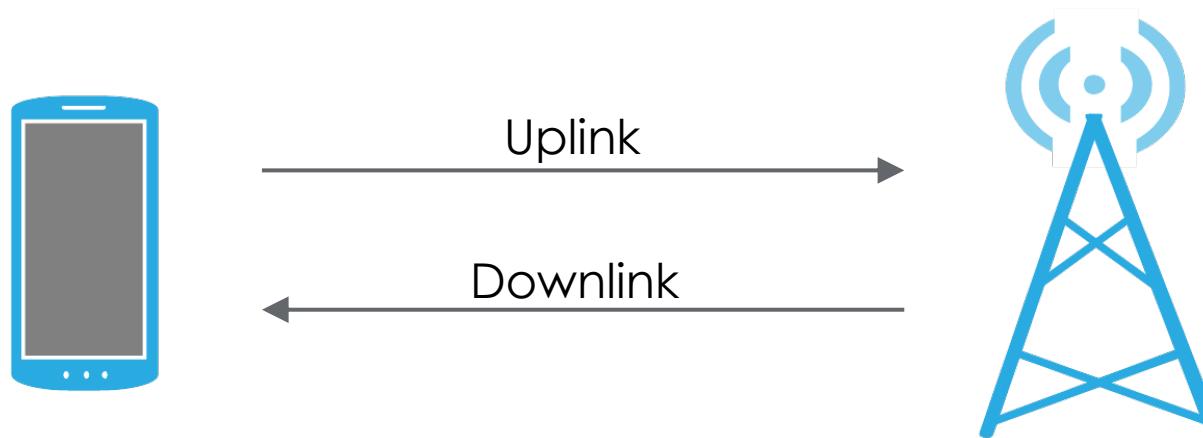
Nowadays, phones concurrently operate on many frequencies (and therefore networks)

- Modern multi-band chips allow a single device to operate on multiple frequency ranges

Channel Allocation

Typically there is a downlink channel and an uplink channel

These channels needs to be spaced in frequency sufficiently far so that they do not interfere with each other



Antenna

There are 2 main types of antennas, each with unique properties

Omnidirectional

- Emits energy in a spherical radius

Directional

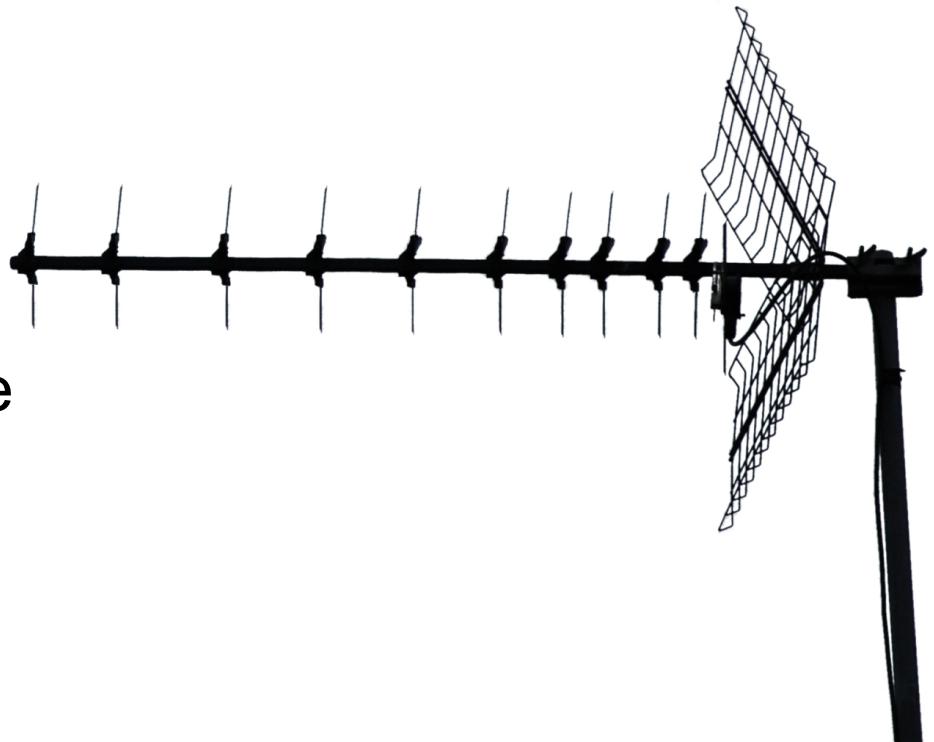
- Emits energy in the shape of the antenna and in the direction and angle at which it is pointed

Directional Antenna

Designed to radiate in a specific direction

- The radiation is focused (see below)

- There are “panel” direction antennas on the front cover of this presentation



Omnidirectional Antenna

Designed to radiate in across a specific plane

- The radiation spreads outward from a center point
- A donut is a reasonable visual

Device Antenna

There are multiple antennas in your mobile device - although some are shared

Designed to transmit and receive at various frequencies

- Cellular (300 MHz - 3 GHz)
- WiFi (Primarily 2.4 GHz, 5 GHz) [there are other odd frequencies specified]
- Bluetooth (2400–2480 MHz)
- NFC (13.56 MHz)

Multiple Antennas

LTE has a feature called Multiple-Input Multiple-Output (MIMO)

Multiple antennas are on the mobile device and are used simultaneously to transmit and receive

- Can significantly increase throughput

Multiple types

- Spatial diversity
- Spatial multiplexing

Further divided:

- SISO - Single in, single out
- SIMO - Single in, multiple out
- MISO - Multiple in, single out
- MIMO - Multiple in, multiple out

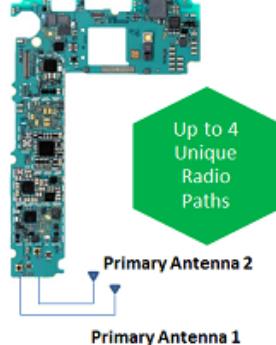
Multiple Antennas

Samsung Galaxy S6 Edge + Antennae Locations



Source: IHS Markit

Diversity Antennae

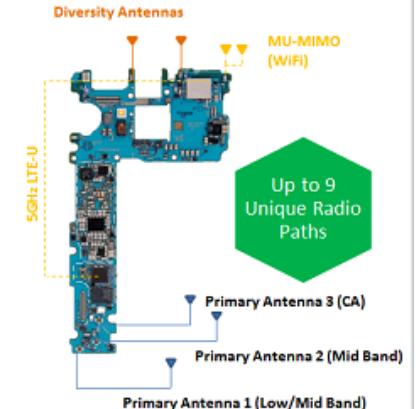


Samsung Galaxy S7 Edge Antennae Locations



Source: IHS Markit

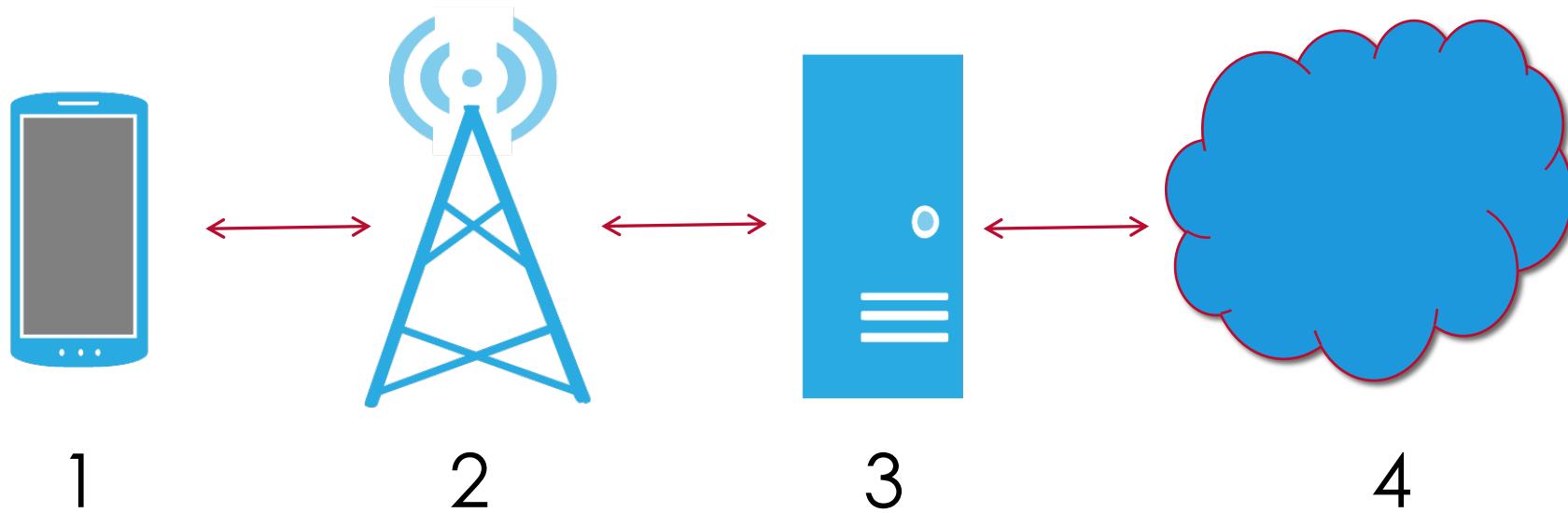
Samsung Galaxy S8 Antennae Locations



Source: IHS Markit

The Big Picture

Mobile devices (1) connect to a base station (2) which connects to a backhaul network (3), which connects to the internet (4).



Network Components

The network between mobile devices and base stations is the Radio Access Network (RAN)

- This name slightly changes with new standards

Base stations are permanent cellular sites housing antennas

Base stations and the backhaul network are run by telco, but there are interconnections and shared sites

- AT&T customers need to be able to contact Verizon (vice versa)

Base stations often connect to backhaul via wired technologies (i.e., fiber)

- Base stations often communicate with each other via wireless

Mobile Devices

These are the devices with wireless radios that connect to cell towers

- Radios are inside phones, tablets, laptops, etc. . .

LTE uses the term User Equipment (UE), previously ~ Mobile Station (MS)

The parts of the UE we are concerned with:

- The handset, aka the ME (Mobile Equipment)
- USIM (Universal SIM)
- Baseband processor

Baseband

Typically a separate processor on the phone

- From companies like Qualcom, Infineon, etc.

Handles all of the telecommunications-related functions

- Sends, receives, processes signals
- Base station and backhaul network communication
- Has direct access to microphone, speakers...

Runs a real time operating system (RTOS)

- Performance matters!
- OSs include ThreadX, Qualcomm's AMSS w/ REX kernel, OKL4

Sometimes shares RAM with application processor (baseband as a modem), sometimes each processor has distinct RAM(shared architecture)

- In a shared configuration the baseband is often the master

May be virtualized

Planes of Communication

Many control systems divide communication into two planes - one for processing information from users and another for how to setup/breakdown the channel and other important functions

Think of this similar to how FTP uses two ports

- TCP port 20 - data
- TCP port 21 - control



Control Plane (CP)

- A private communication channel that is distinct from data the UE operator can influence
- Used to send control messages to components
- Mobile users should not be able to influence this in any way

User Plane (UP) signaling

- Voice and data information

Cellular networks use this design extensively

Packets and Circuits

Pre-LTE, cellular networks used circuit switching technology for voice

- LTE uses VoLTE which is VoIP over LTE
- Not implemented currently, calls fall back to previous networks

Data traffic is sent over nearly distinct interconnected packet switching networks

- GSM first used GPRS, then moved to EDGE
- UMTS used HSPA technologies including HSPA+

Since LTE is completely IP based, it does not use circuits (sort of... e.g. GTP Tunnels)

Network Interconnection

Circuit switched networks need to be able to connect with packet switched networks and other distinct cellular networks

- The internet is a good example
- This is a complex process

GPRS (General packet radio service)

- 2.5G packet switched technology

EDGE (Enhanced Data Rates for GSM Evolution)

- 2.75G packet switched technology

HSPA (High Speed Packet Access)

- 3.5/3.75 packet switched data technology
- There were a few quick iterations on this technology, thus “variants”

Attachment, Handoff, & Paging

The first step in a mobile device connecting to a network is referred to as network attachment

- Mobile devices request network access to a base station, which passes this request onto the backhaul network
- Authentication of the mobile device is then performed

If a mobile device is moving (such as on a freeway) a call will need to be transferred from one base station to another

- This is called handoff
- This is a very common, yet is complex, process

Paging is the process of how a backhaul network locates and directs calls a mobile device

- Base stations provide a list of active devices to the backhaul

Connection Management

EPS (Evolved Packet System) Connection Management (ECM)

- describes the signalling connectivity between the UE and the EPC

UE related information is released after a certain period of time without use or connection

ECM-states

- ECM-CONNECTED
- ECM-IDLE

TS 23.401 for more information

Subscriber Identity

GSM, UMTS, and LTE all contain a unique ID for a cellular subscriber

- International Mobile Subscriber Identity (IMSI)
- 15 digit number stored on the SIM

Consists of 3 values: MCC, MNC, and MSIN

- Possibly a software version (SV) appended (IMSI-SV)

Mobile Country Code (MCC) - Identifies the country

Mobile Network Code (MNC) - Identifies the network

Mobile Subscriber ID number (MSIN) - Identifies a user

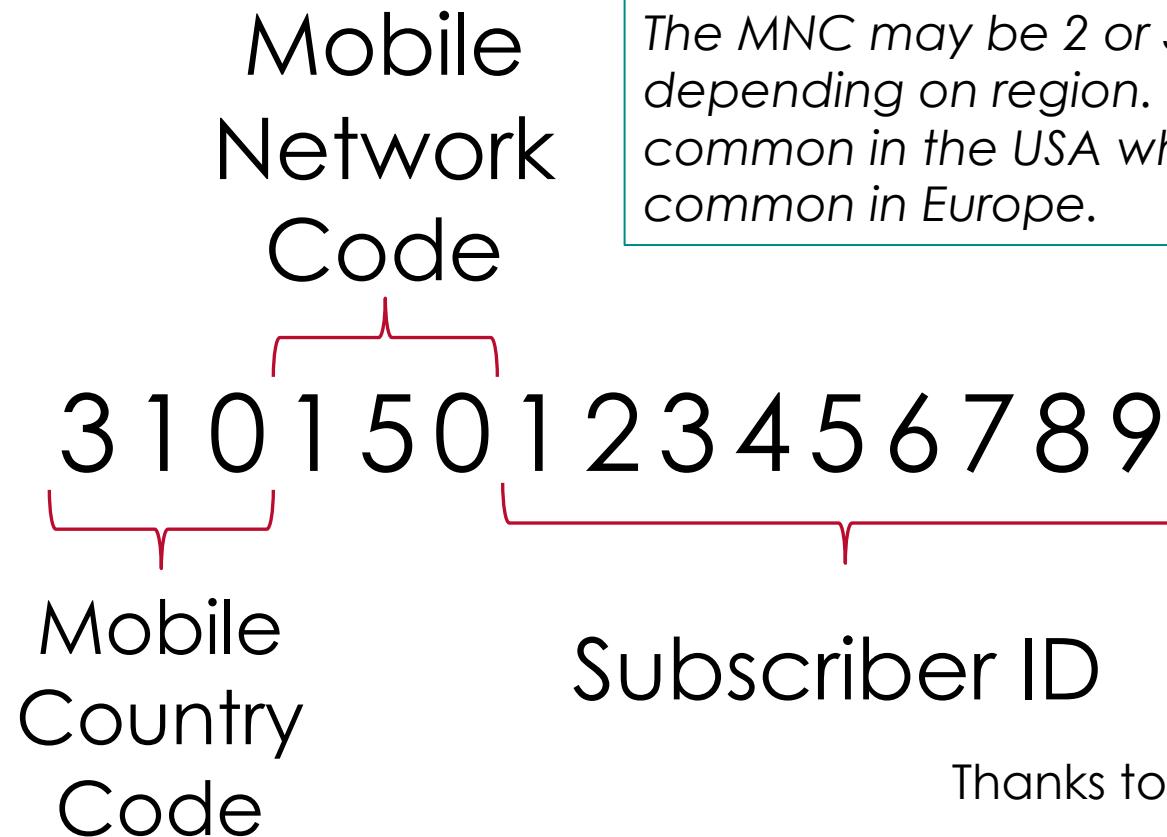
Temporary identities also exist

- Temporary Mobile Subscriber Identity (TMSI)
- Globally Unique UE Identity (GUTI)

This information is stored on the SIM/USIM

Mobile Subscriber ISDN Number (MSISDN) – The phone number, which is distinct from the MSIN

IMSI Example



Thanks to [Wikipedia](#) for the sample IMSI

Terminal Identity

GSM, UMTS, and LTE all contain a unique ID for a terminal ME/UE

- International Mobile Equipment Identity (IMEI)

It is 16 digits with the first 14 indicating equipment identity

- The last 2 indicates software version (SV)
- Referred to as IMEISV

Dial *#06# to display your IMEI

Illegal in some countries to change a phone's IMEI

SIM Cards

A removable hardware token used for GSM, UMTS, and LTE

- Verizon is changing to LTE and is also using the hardware token

Over 7 billion SIMs in circulation

Houses a processor and runs an OS

Java Card runs atop the OS, which is a type of Java Virtual Machine (JVM) for applications

Stores cryptographic keys and sometimes SMSs and contacts

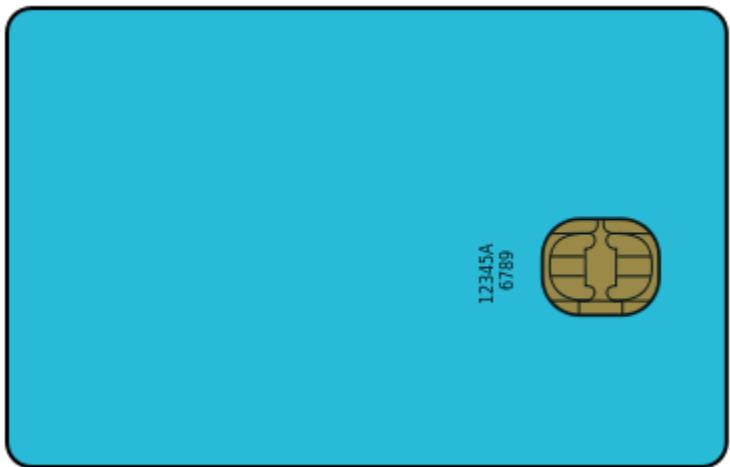
SIM application toolkit (STK) is used to create mobile applications

SIMs are deprecated – the modern term is USIM

- The USIM runs atop the UICC which is the physical card

SIM Card

Full-size SIM



Micro-SIM



Mini-SIM



Nano-SIM

From left to right, we are only removing plastic. The integrated circuit remains static.

Thanks to [Wikipedia](#)

3GPP

An international standards body

Evolves and/or standardizes GSM, UMTS, LTE among others

From their page:

The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the highly successful Reports and Specifications that define 3GPP technologies

We will primarily discuss 3GPP standards

Other standards exist from a distinct standards body known as 3GPP2

- CDMA2000 and the now deprecated UMB

Major Standards

Multiple standards bodies involved

GSM

Standards grow and evolve from one another

CDMA

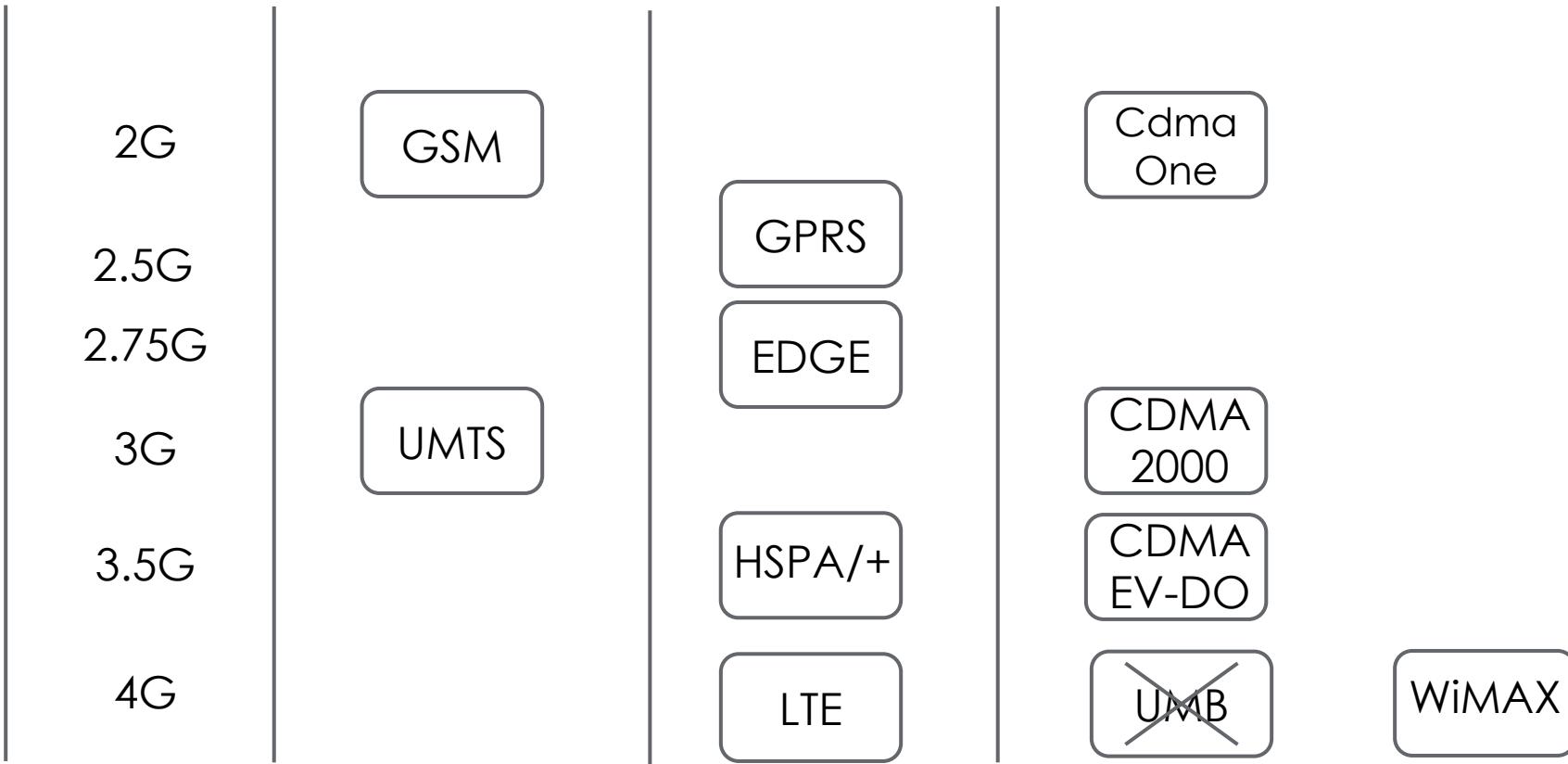
UMTS

EV – DO

WiMAX

LTE

Cellular Standards



A Note on 3GPP

LTE is a 3GPP specification

- Therefore we will be discussing 3GPP specifications in depth

We will introduce GSM

We will then build on these concepts from GSM to UMTS to LTE

Packet switched technologies will be discussed as well

WiMax Forum standards are not included

GSM

Global System for Mobile Communications

2G digital voice

Air interface: TDMA

- Multiple users on the same channel

Operates at various spectrums worldwide

There are 4 separate systems:

- Base station subsystem (BSS)
- Network subsystem (NSS)
- Operations and support subsystem (OSS)
- Mobile station subsystem (MSS)

Each subsystem has a distinct purpose

GSM Components Description

Mobile station subsystem (MSS)

- Mobile handset and SIM

The base station subsystem BSS consists of a controller and transceiver

- Base station transceiver (BTS) is the cell tower
- Base station controller (BSC) controls 1 or more BTSs
- Housed at the Mobile Telephone Switching Office (MTSO)

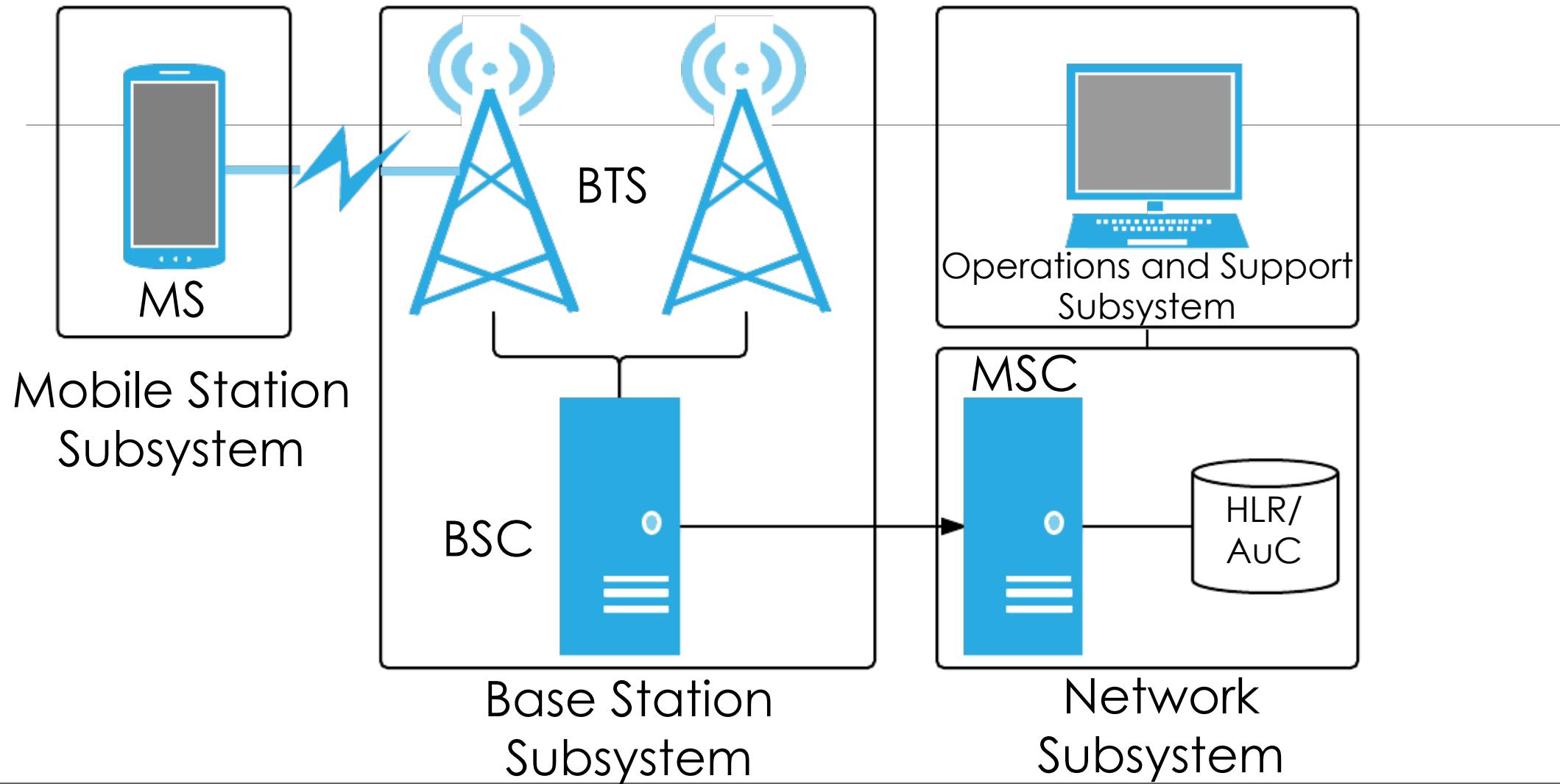
Network subsystem (NSS):

- MSC (Mobile Switching Center) and MTSO
- MTSO-switch connects cell network to PSTN
- MTSO houses the HLR, which supports the AuC

Operations and Support (OSS)

- Manages the network as a whole

GSM Architecture Diagram



UMTS

Universal Mobile Telecommunications System

3G digital voice

Air interface: W-CDMA

Operates at various spectrums worldwide

UMTS Components

Consists of the core network (CN), Universal Terrestrial Radio Access Network (UTRAN), and UE

Runs 2G circuit switched and 3G packet switched components concurrently - it looks confusing at first

The UTRAN contains:

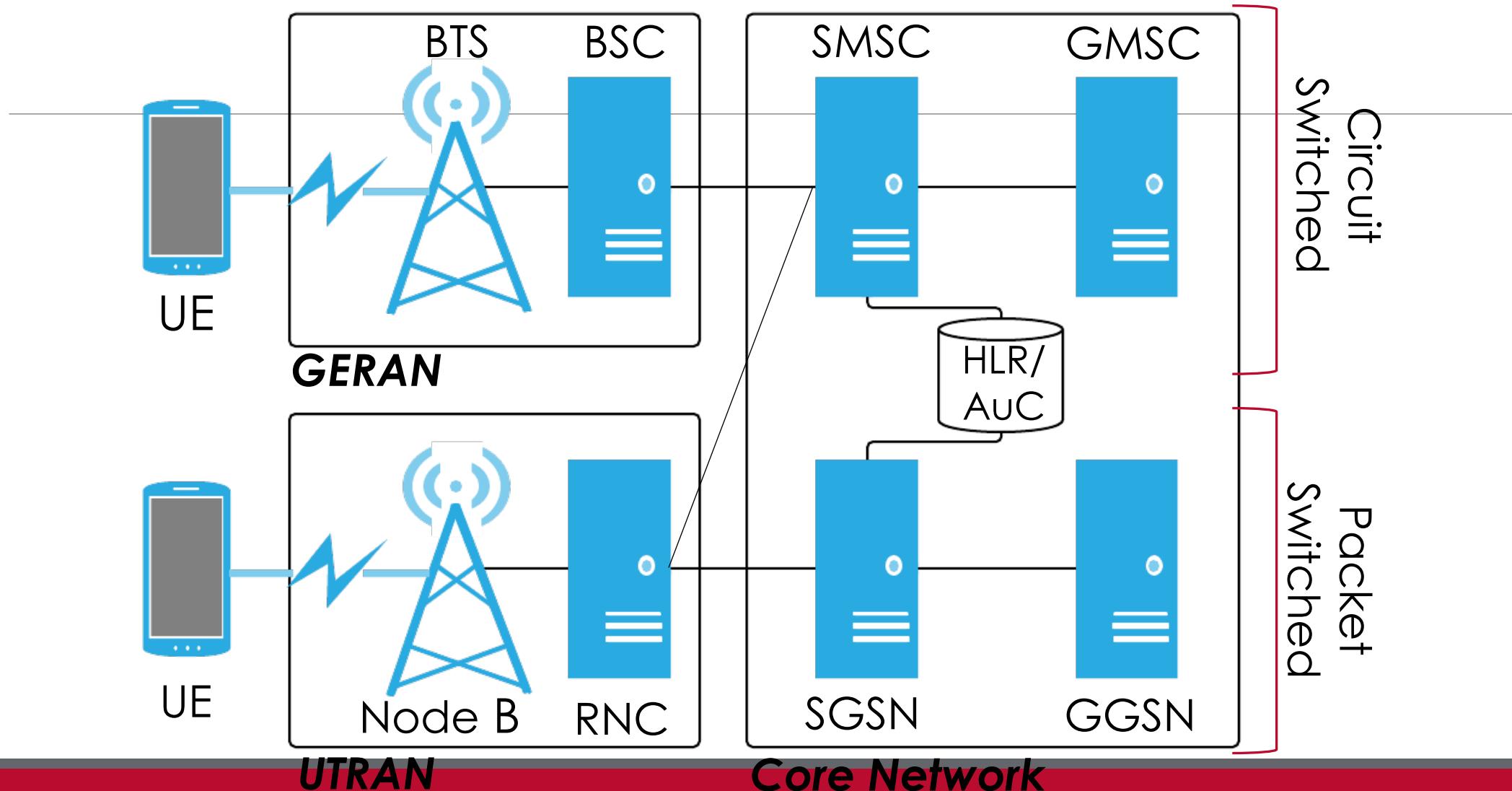
- Node B (think of the phone as Node A)
- Radio Network Controller (RNC)

The CN contains:

- Serving Mobile Switching Center (GMSC)
- Gateway Mobile Switching Center (GMSC)
- Serving GPRS support node (SGSN)
- Gateway GPRS support node (GGSN)
- Home Location Register/Authentication Center (HLR/AuC)

We are not discussing GPRS-related nodes

UMTS Architecture Diagram



UMTS & GSM Compatibility

UMTS was designed to work concurrently with GSM

2G SIMs were included

Much of the terminology is slightly modified

- BTS -> Node B

LTE

Long Term Evolution

- Also known as the Evolved Packet System (EPS)

4G data **and** voice technology

Air interface: OFDMA

3 main components:

- Evolved U-TRAN (E-UTRAN) - Radio Network
- Evolved Packet Core (EPC) - Backhaul
- IP Multimedia Subsystem (IMS) - Extended backhaul functionality

Remember: LTE is a completely packet-switched technology for both data and voice

- LTE can fall back to older networks for voice (Circuit-switched fallback)

VoLTE (voice over LTE)

- To activate voice calls over LTE (using IP Multimedia Subsystem)
- Active in Italy from end of 2015 (Vodafone, TIM)

LTE Components

User equipment (UE)

Evolved Node B (eNodeB)

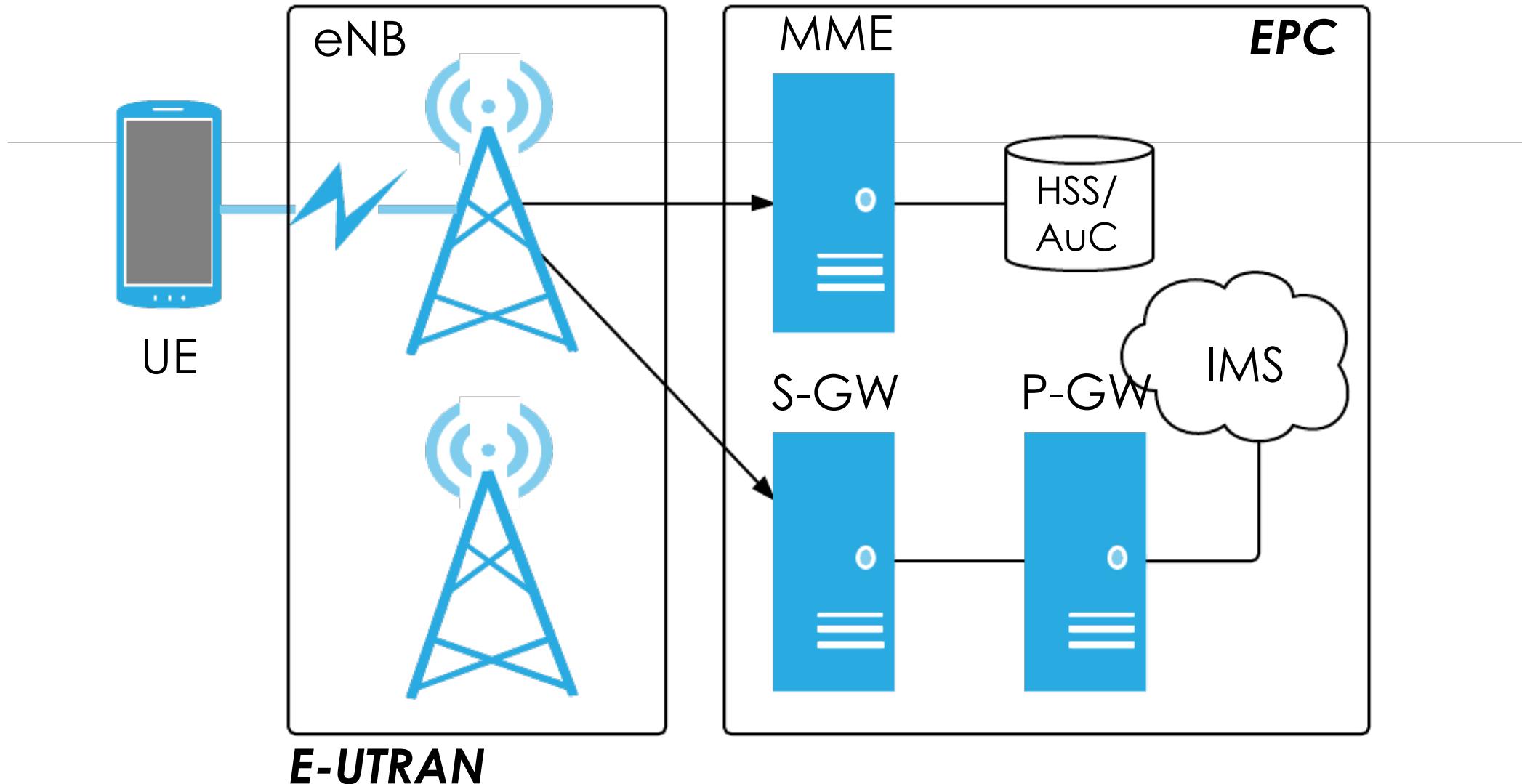
Mobility Management Entity (MME)

Serving Gateway (S-GW)

Packet Data Network Gateway (P-GW)

Home Subscriber Server (HSS)

LTE/EPS Architecture Diagram



LTE Components Description

User equipment (UE) – The LTE device

Evolved Node B (eNodeB or eNB) – An evolved Node B (BTS)

E-UTRAN - The radio network that exists between UEs and eNBs

Mobility Management Entity (MME) – Primary signaling node (no user traffic). Large variation in functionality including managing/storing UE contexts, creating temporary IDs, sending pages, controlling authentication functions, and selecting the S-GW and P-GWs

Serving Gateway (S-GW)- Carries user plane data, anchors UEs for intra-eNB handoffs, and routes information between the P-GW and the E-UTRAN

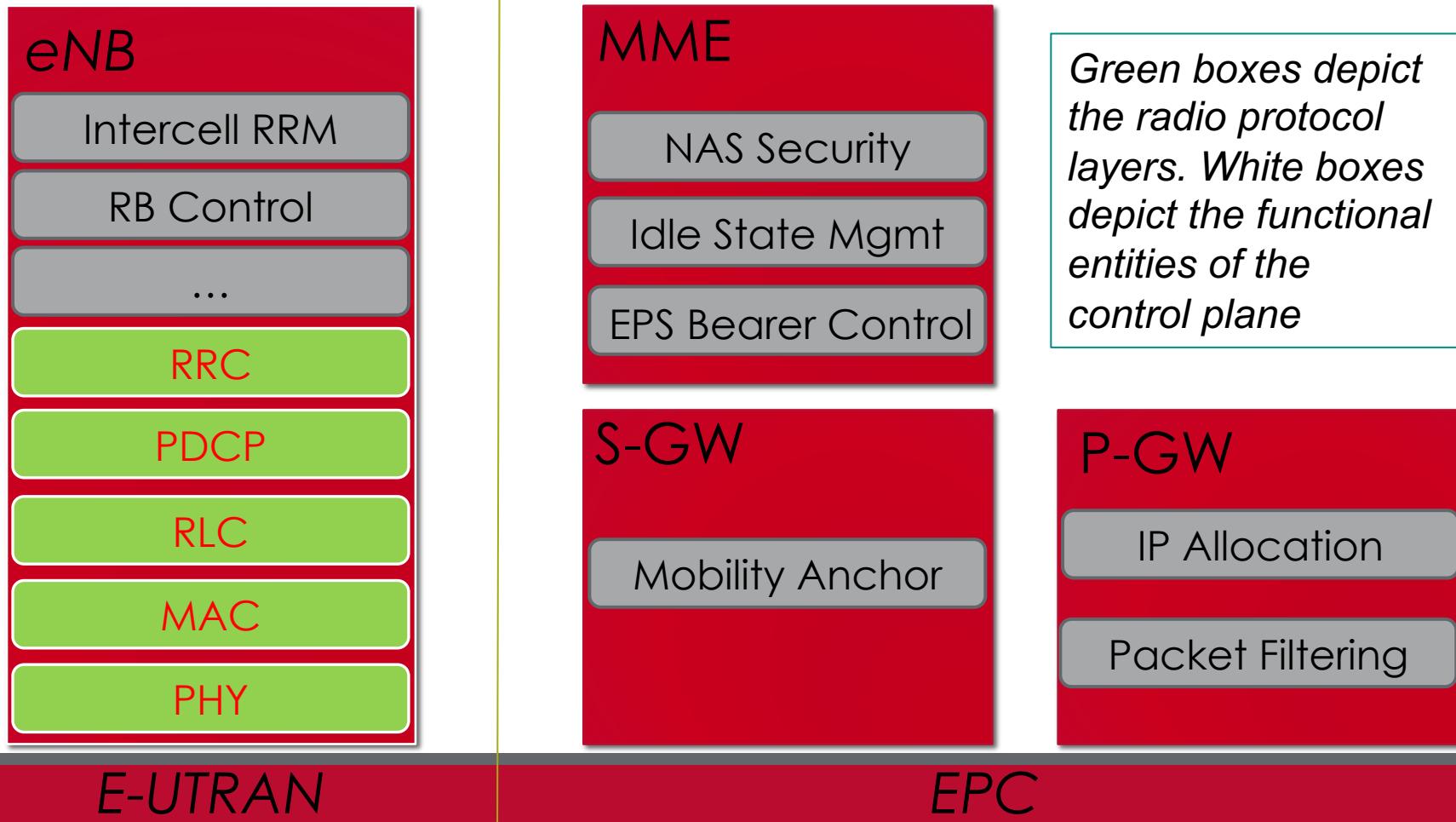
Packet Data Network Gateway (P-GW) – Allocates IP addresses, routes packets, and interconnects with non 3GPP networks

Home Subscriber Server (HSS) - This is the master database with the subscriber data

Authentication Center (AuC) - Resides within the HSS, maps an IMSI to K, performs cryptographic calculations during AKA

IP Multimedia Subsystem (IMS) – Paging, connections to the PSTN, and support for VoLTE

E-UTRAN & EPC Protocols



Protocol Discussion

There are a number of additional capabilities provided by the eNB

- IP header compression of user data stream
- Selection of an MME at UE attachment when no routing to an MME can be determined from the information provided by the UE
- Routing of User Plane data towards Serving Gateway

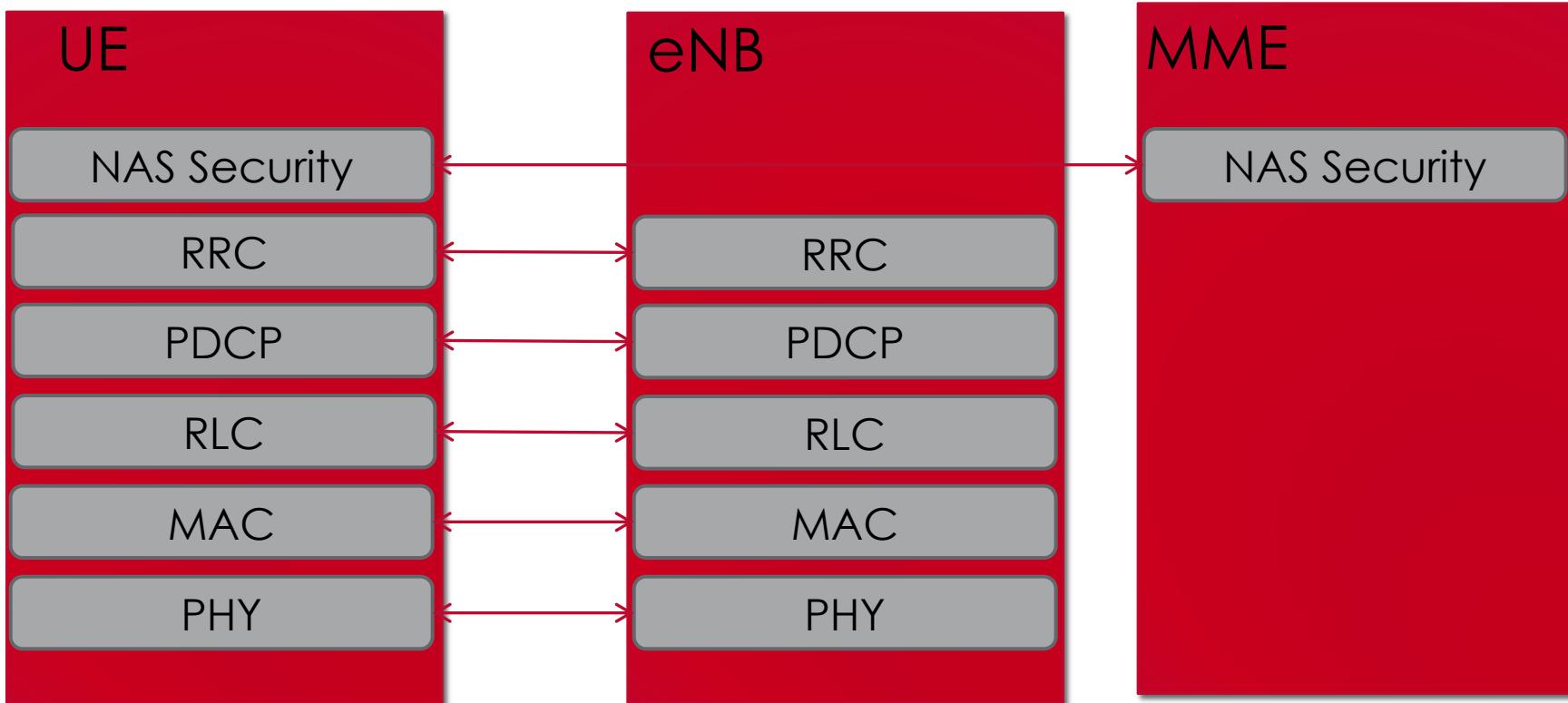
Radio Resource Control (RRC) – Transfers NAS messages, AS information may be included, signaling, and ECM

Packet Data Convergence Protocol (PDCP) – header compression, radio encryption

Radio Link Control (RLC) – Readies packets to be transferred over the air interface

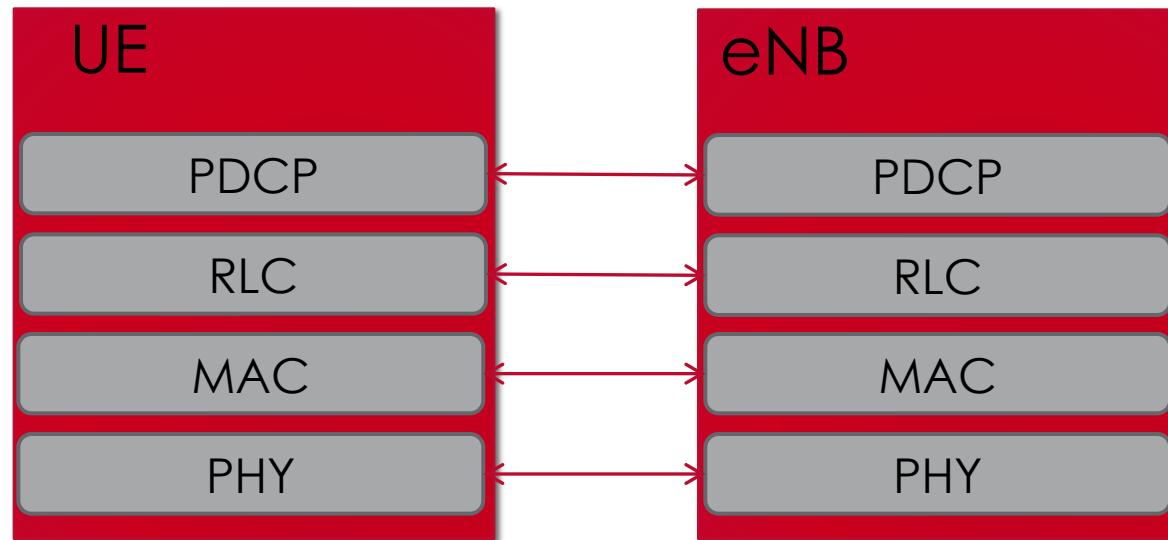
Medium Access Control (MAC) – Multiplexing, QoS

Control Plane Protocols



Adapted from [3GPP TS 36.300](#)

User Plane Protocols



Adapted from [3GPP TS 36.300](#)

Interfaces

Interfaces are the communications paths LTE components use to communicate

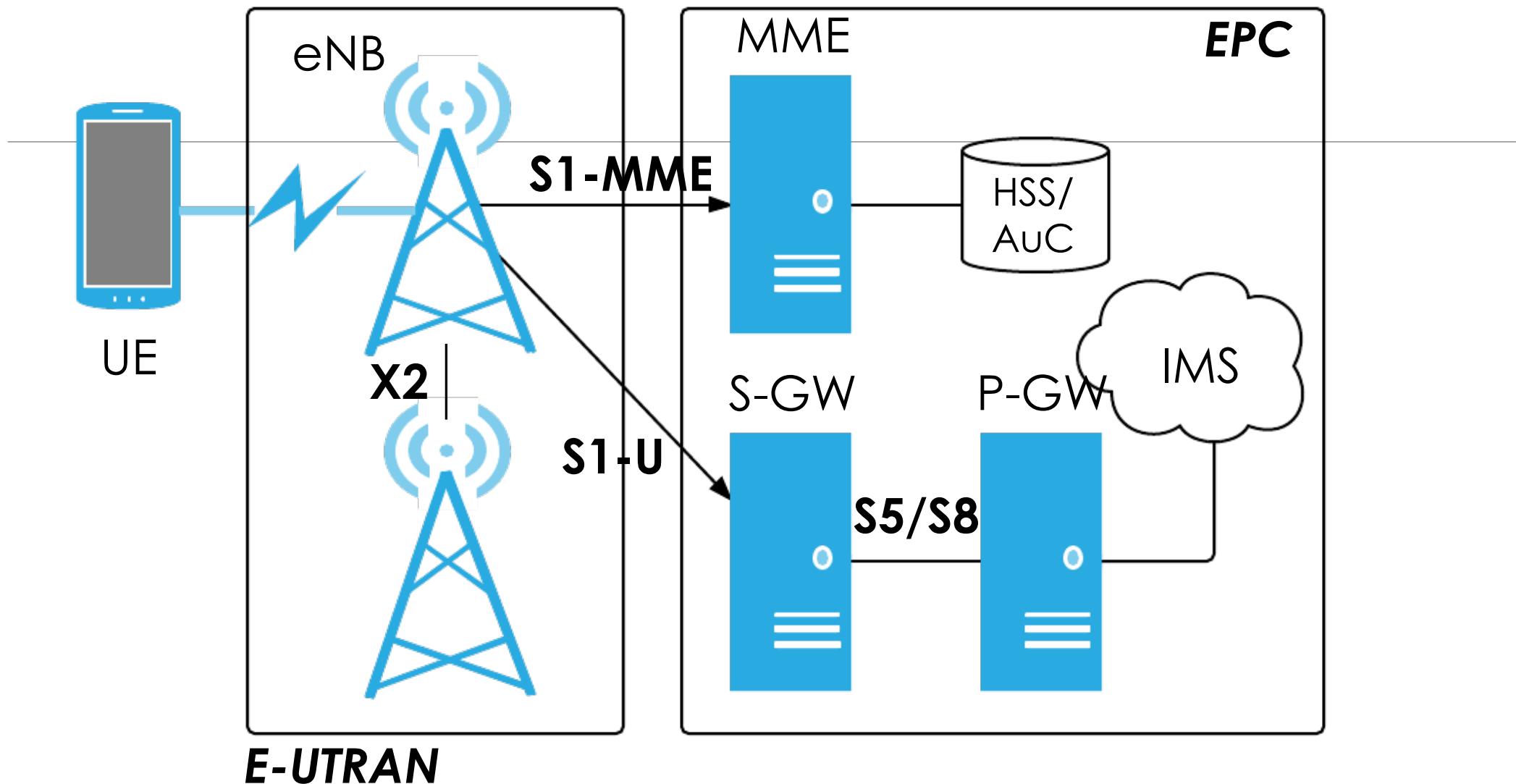
Each one is provided with its own label

- There may be unique protocols between various interfaces

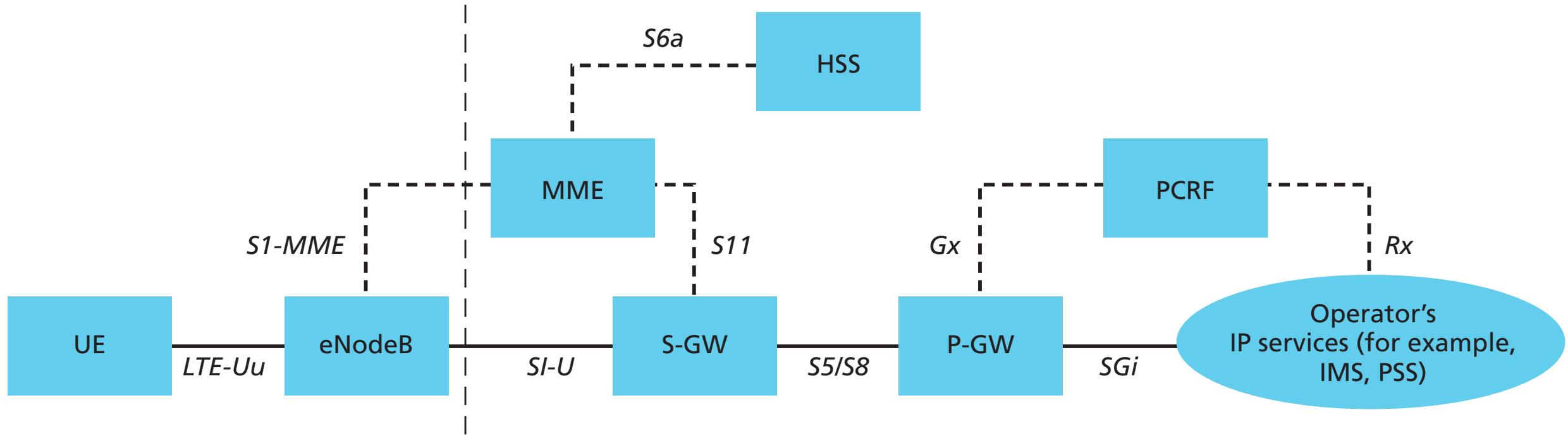
There are many interfaces - we are discussing a subset

- X2 - eNB to eNB
- S1-U - eNB to S-GW
- S1-MME (sometimes S1-C) - eNB to MME
- S5/S8 - S-GW to P-GW

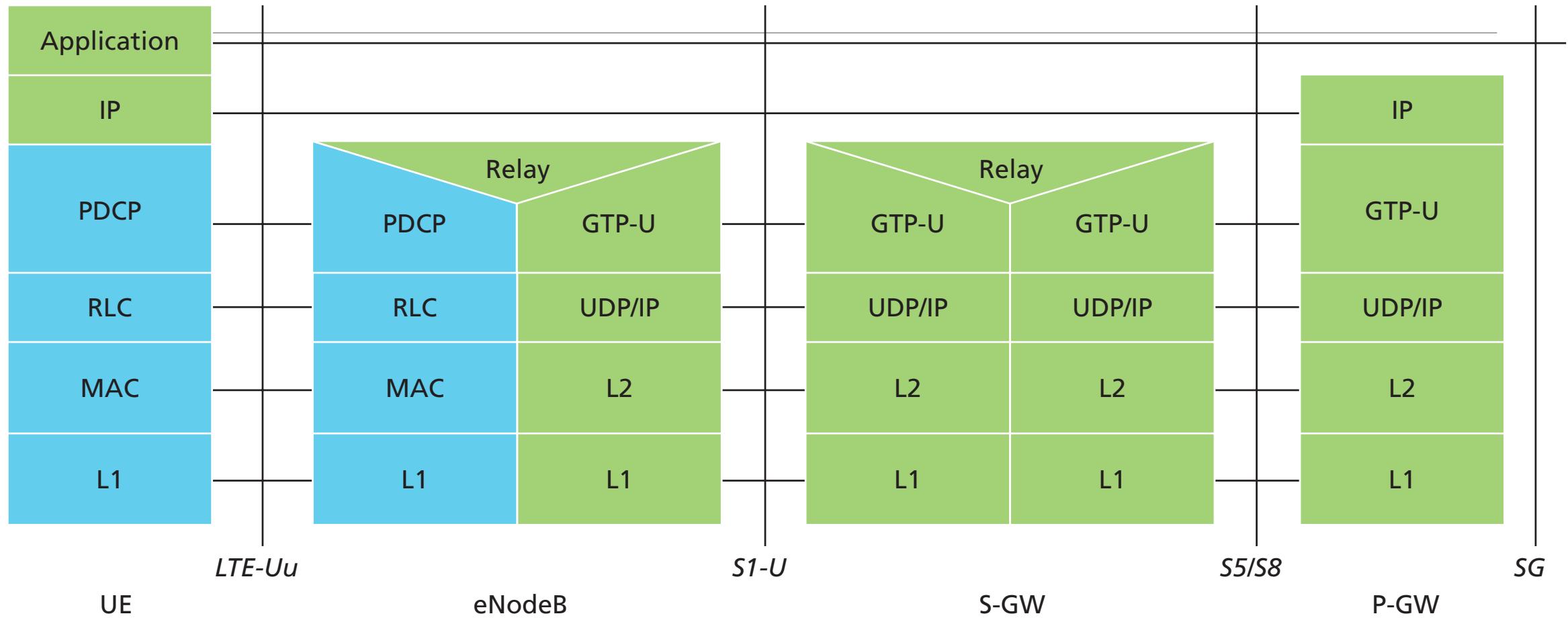
LTE/EPS Interface Diagram



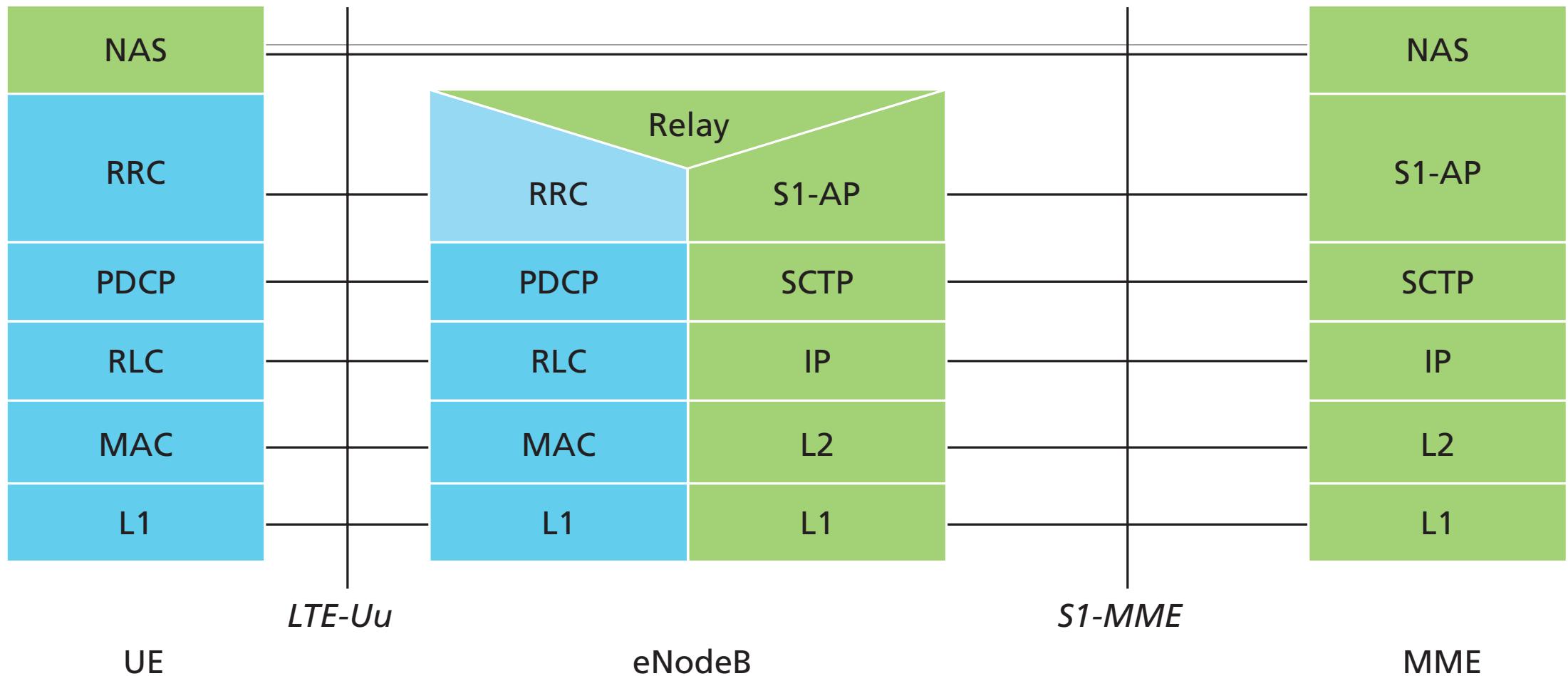
LTE Evolved Packet System



LTE E-UTRAN User space protocols



LTE E-UTRAN Control space protocols



LTE PHY Basics

- Six bandwidths
 - 1.4, 3, 5, 10, 15, and 20 MHz
- Two modes
 - FDD and TDD
- 100 Mbps DL (SISO) and 50 Mbps UL
- Transmission technology
 - OFDM for multipath resistance
 - DL OFDMA for multiple access in frequency/time
 - UL SC-FDMA to deal with PAPR ratio problem

LTE in Italy

TIM:

- 800 MHz (B20), 1800 MHz (B3), 2600 MHz (B7);

Vodafone:

- 800 MHz (B20), 1800 MHz (B3), 2600 MHz (B7);

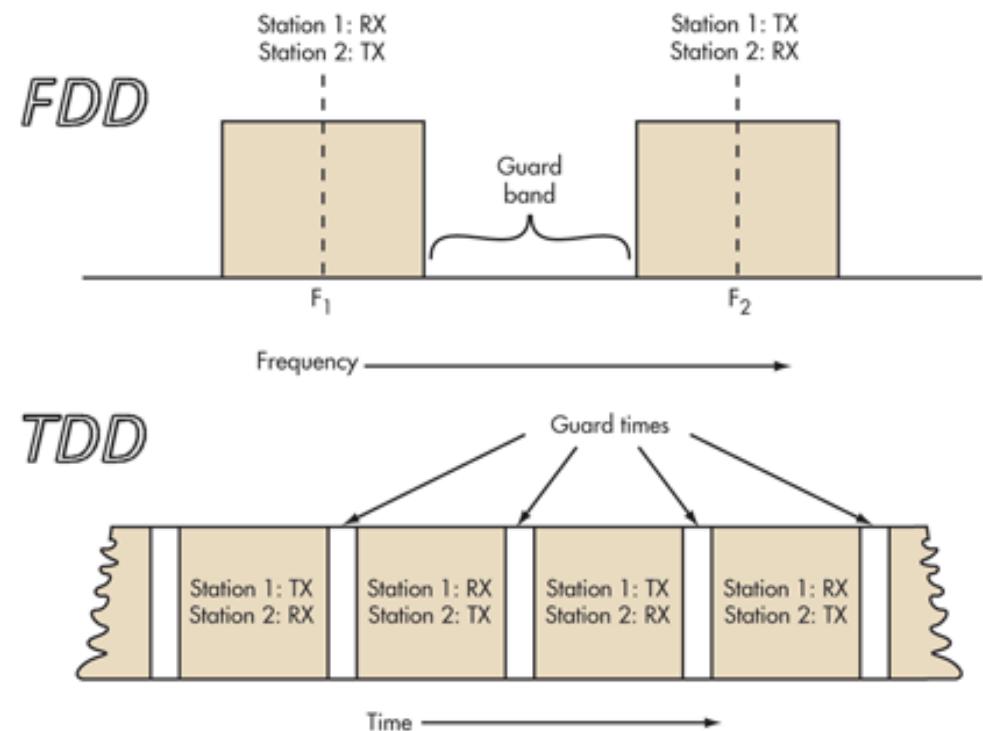
Wind:

- 800 MHz (B20), 2600 MHz (B7);

3 Italia:

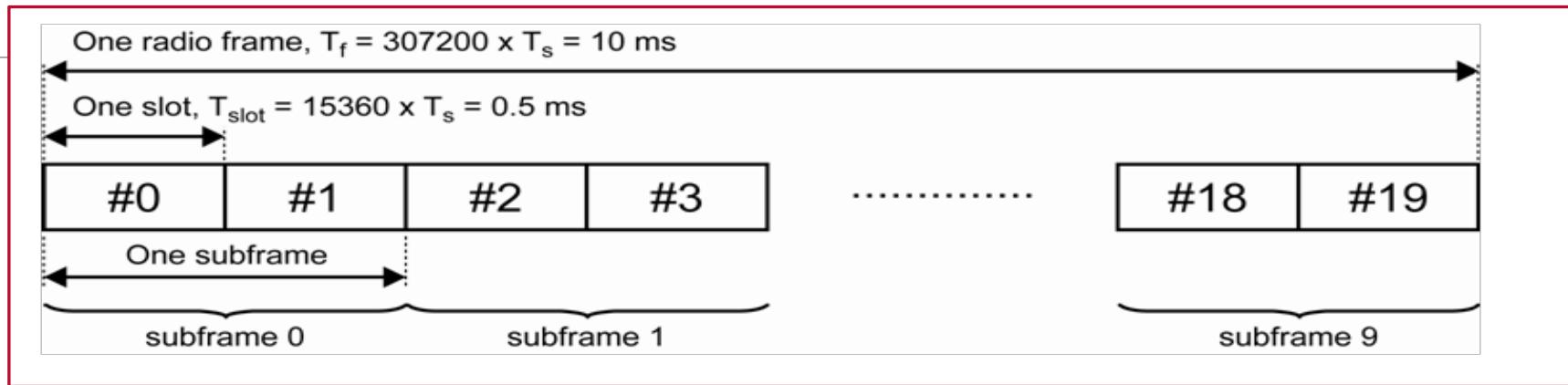
- 1800 MHz (B3), 2600 MHz (B38, TDD-LTE)

FDD is most popular duplexing

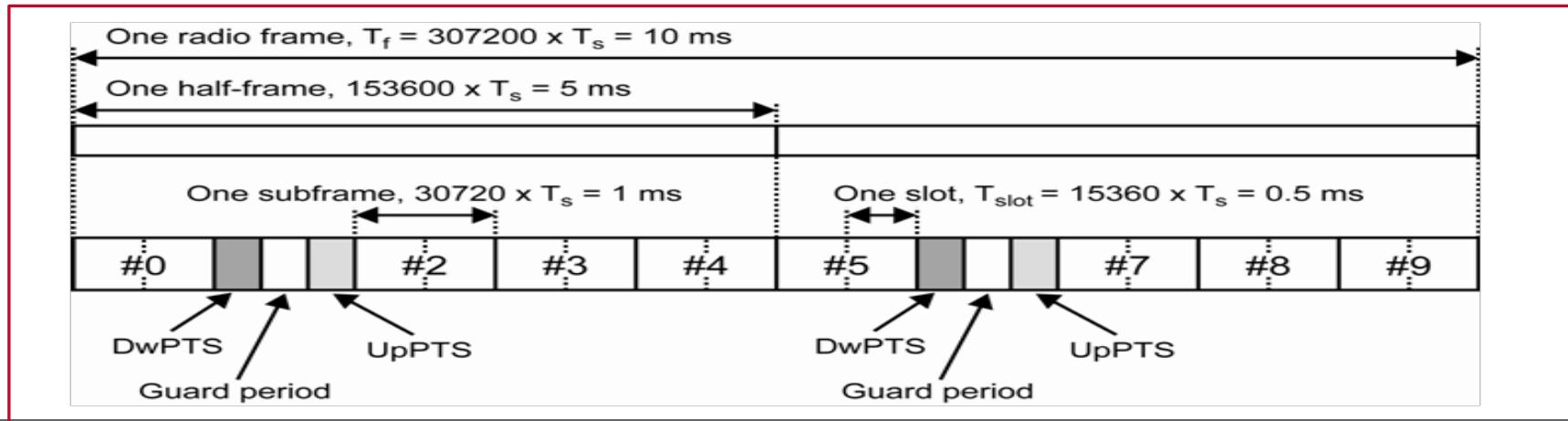


LTE Frame structure

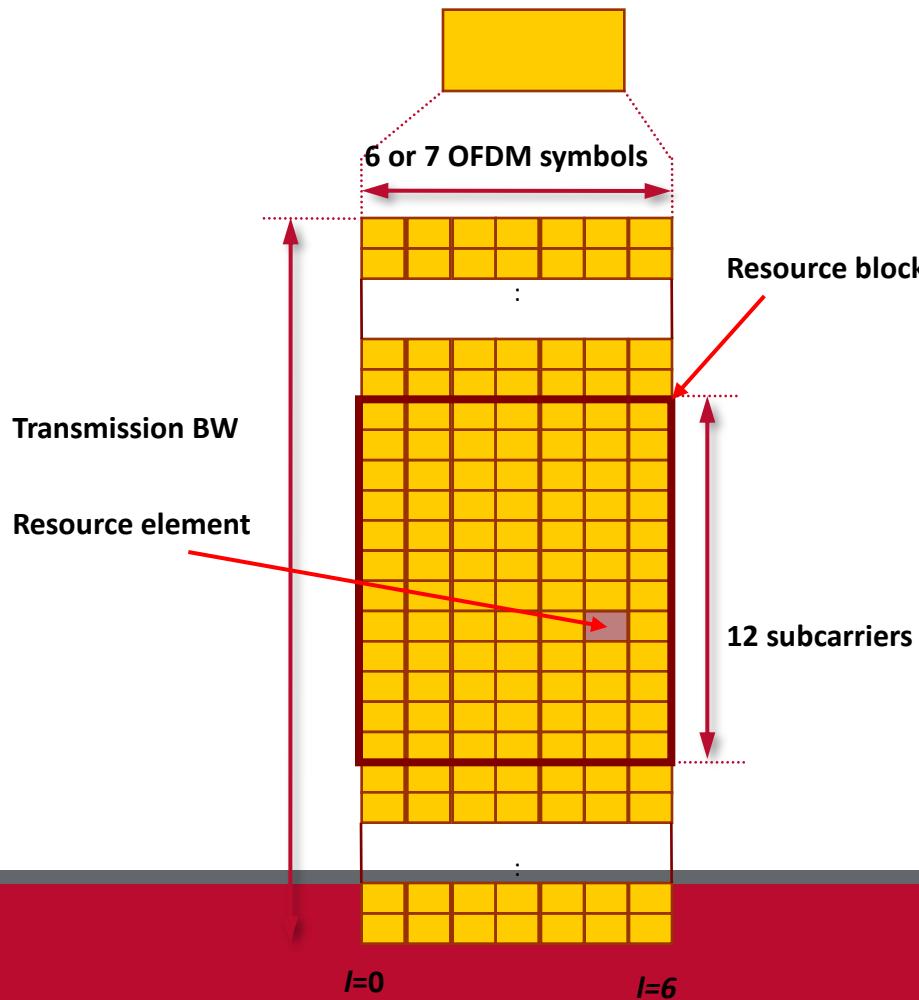
Frame Structure Type 1 (FDD)



Frame Structure Type 2 (TDD)



LTE Resource grid



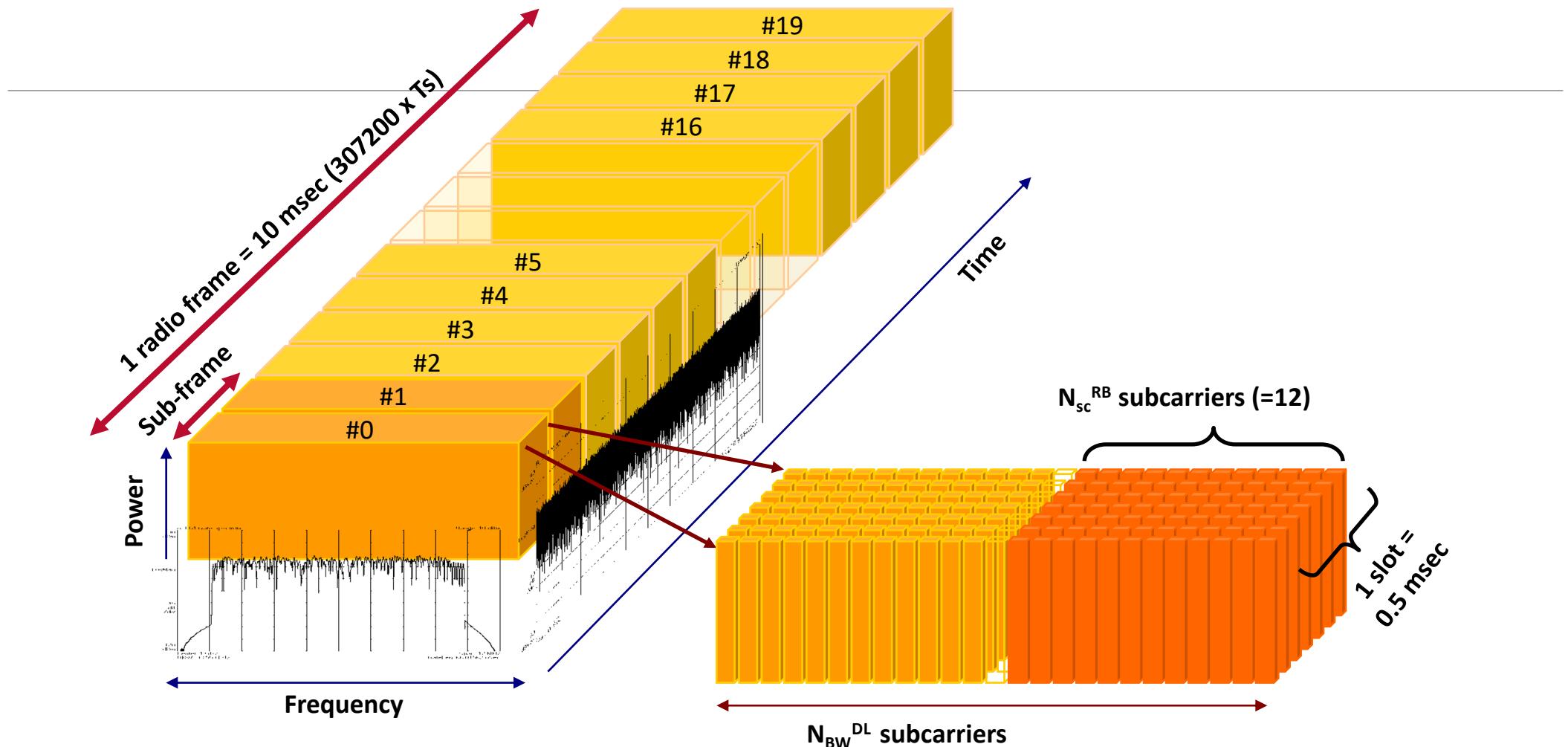
6 or 7 OFDM symbols in 1 slot

Subcarrier spacing = 15 kHz

Block of 12 SCs in 1 slot = 1 RB

- $0.5 \text{ ms} \times 180 \text{ kHz}$
- Smallest unit of allocation

LTE 2D Time and Freq. grid



LTE DL PHY Channels

Signals: generated in PHY layers

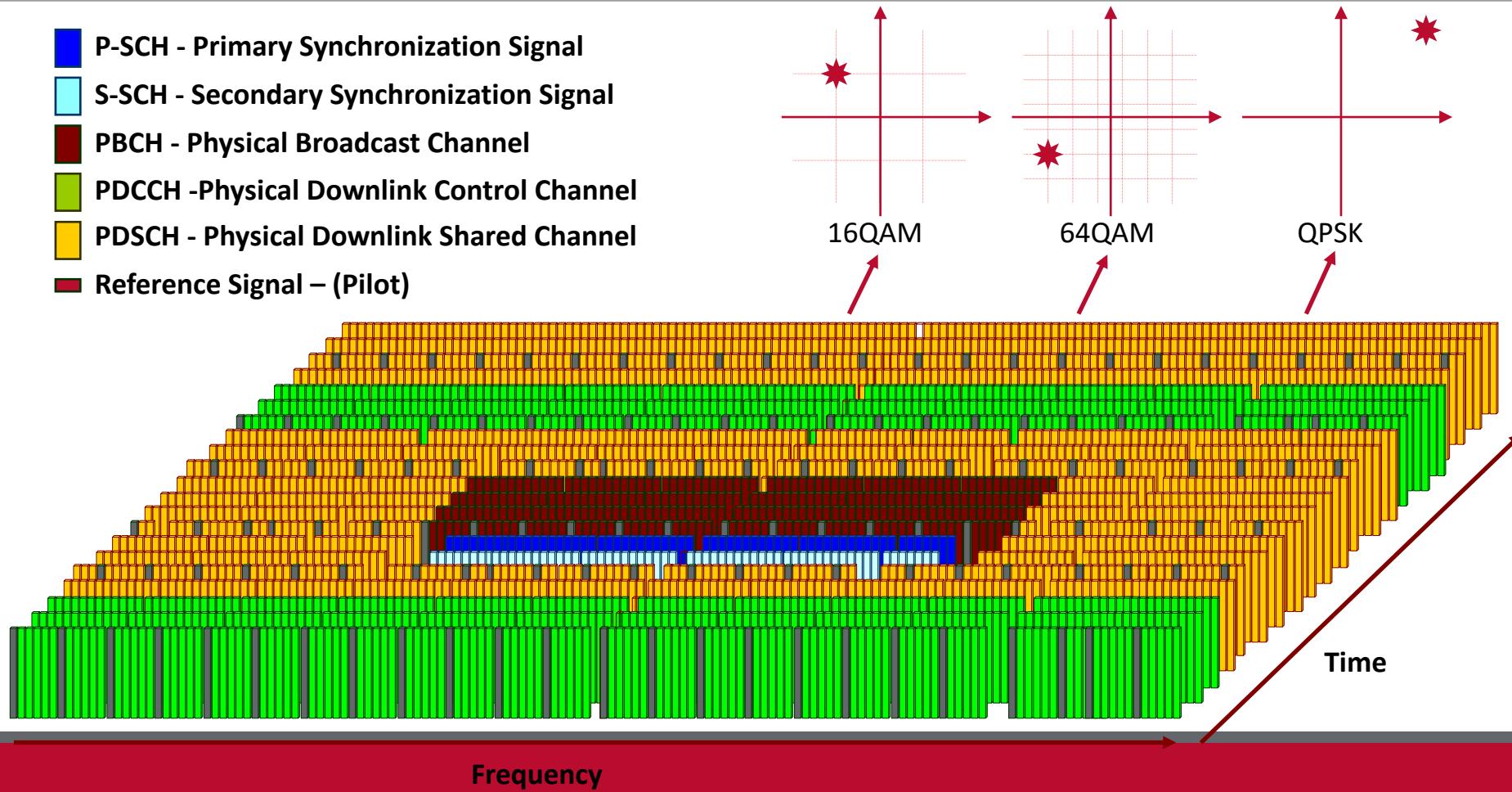
- P-SS: used for initial sync
- S-SS: frame boundary determination
- RS: pilots for channel estimation and tracking

Channels: carry data from higher layers

- PBCH: broadcast cell-specific info
- PDCCH: channel allocation and control info
- PCFICH: info on size of PDCCH
- PHICH: Ack/Nack for UL blocks
- PDSCH: Dynamically allocated user data

LTE DL PHY Channels Mapping

- P-SCH - Primary Synchronization Signal
- S-SCH - Secondary Synchronization Signal
- PBCH - Physical Broadcast Channel
- PDCCH -Physical Downlink Control Channel
- PDSCH - Physical Downlink Shared Channel
- Reference Signal – (Pilot)



LTE UL PHY Channels

Signals: generated in the PHY layer

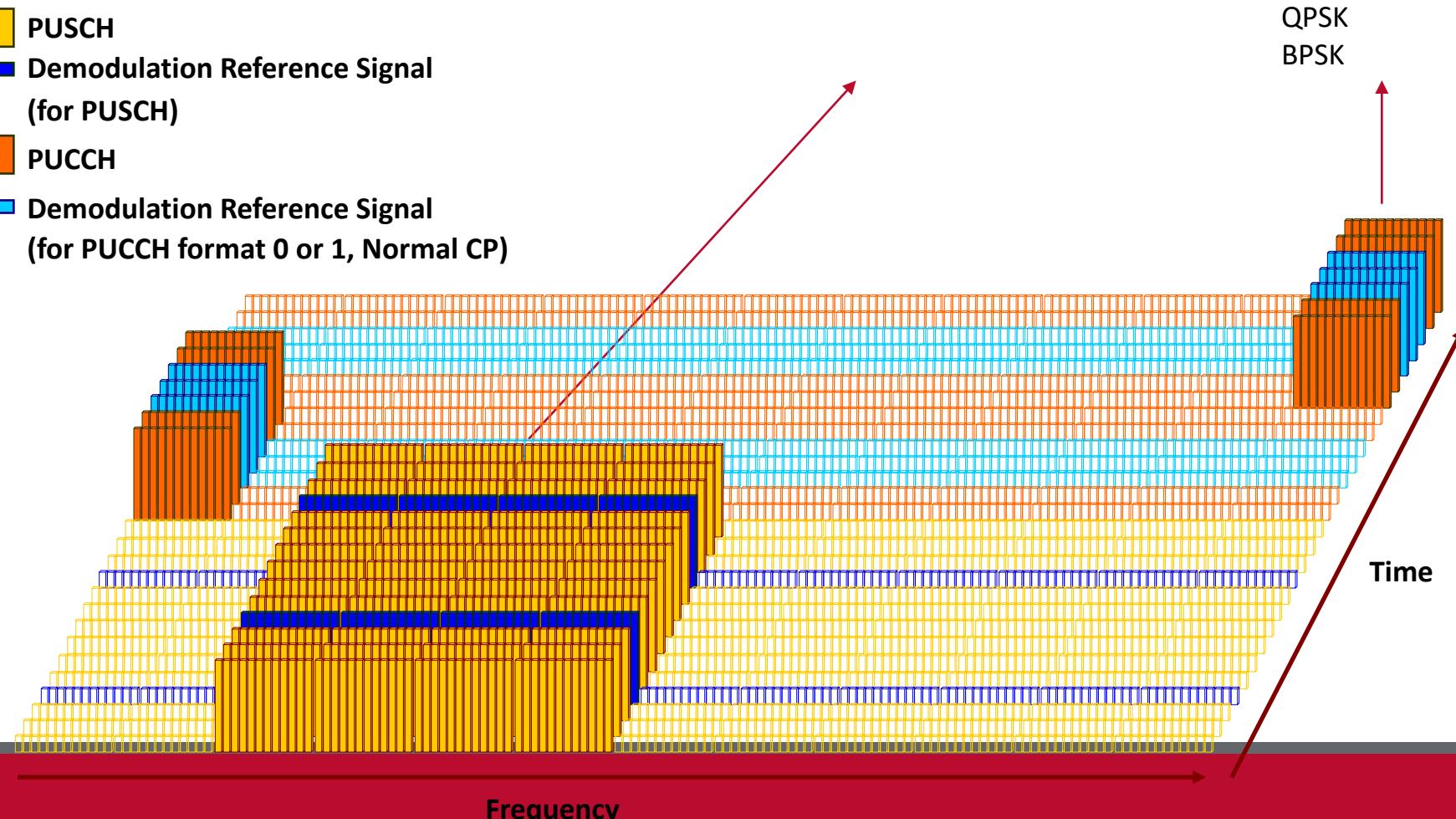
- Demodulation RS : sync and channel estimation
- SRS: Channel quality estimation

Channels: carry data from higher layers

- PUSCH: Uplink data
- PUCCH: UL control info
- PRACH: Random access for connection establishment

LTE DL PHY Channels Mapping

- PUSCH
- Demodulation Reference Signal (for PUSCH)
- PUCCH
- Demodulation Reference Signal (for PUCCH format 0 or 1, Normal CP)



Resources & References

- Muyung, [A Technical Overview of 3GPP LTE](#)
- [TS 36.300](#) – Overall description of E-UTRAN